

ABSTRACT

A method of manufacturing devices that generate digital signatures such that each device may be reliably and uniquely identified includes creating a public-private key pair within each device during manufacture; exporting only the public key from the device; 5 retaining the private key within the device against the possibility of divulgement thereof by the device; and securely linking said exported public key with other information within the environment of the manufacture of the device, whereby each device is securely bound with its respective public key. A database of PuK-linked account information of users is maintained. The PuK-linked account information for each user includes a public key of 10 such a device; information securely linked with the public key during manufacture; and third-party account identifiers, each of which identifies an account to a third-party of the user maintained with the third-party that has been associated with the user's public key by the third-party.